

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

#### REMARKS

In view of the following remarks, the Applicant respectfully requests reconsideration of the present application.

#### Objections and Rejections

The Office Action dated December 29, 2005:

1. rejects claims 1-29 on the ground of nonstatutory obviousness-type double patenting over claims 1-41 of copending Application Serial No. 09/655,230 ("the '230 patent application") which issued March 28, 2006, as United States Patent no. 7,020,282 B1 ("the '282 patent"); and
2. rejects claims 1-29 under 35 U.S.C. § 103(a) as being unpatenably obvious in view of the Crandall patent.

#### Argument

##### **Claims 1-29 Traverse Rejection for Obviousness-Type Double Patenting**

In explaining the obviousness-type double patenting rejection of claims 1-29 the December 29, 2006, Office Action states on page 2 that:

[a] nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

claim(s) because the examined application claim is either anticipated by or would have been obvious over, the reference claim(s).

Attached hereto as Exhibits B and C are copies of the filing receipts respectively for the patent application identified above, and for the '230 patent application. As is readily apparent from Exhibits B and C, both patent applications were filed on the same day, i.e. September 5, 2000. Since the present patent application and the patent application which issued as the '282 patent were filed on the same day:

1. under 35 U.S.C. § 102 neither patent application is prior art to the other patent application; and
2. therefore due to the preceding statutory impediment claims in either patent application cannot anticipate or render obvious a claim in the other patent application.

Furthermore, Applicant fails to find in the December 29, 2005, an element-by-element comparison between a single claim pending in this patent application and an issued claim in the '282 patent. Therefore, Applicant respectfully submits that the December 29, 2005, Office Action fails to establish a prima facie basis for rejecting any claim pending in the present patent application based upon the nonstatutory ground of obviousness-type double patenting over any claim in the '282 patent.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

Attached hereto as Exhibit D is a comparison between the texts of independent claims respectively of the '230 patent application and of the present patent application. Exhibit D demonstrates that, in comparison with the independent claims of the '230 patent application, this patent application's independent claims presently include additional method steps, and omit method steps. Differences between the texts of independent claims respectively of the '230 patent application and of the present patent application arise inherently from differences in the quantities which the two patent applications respectively disclose as being:

1. stored into the publicly accessible repository; and
2. computed using quantities retrieved from the publicly accessible repository.

The differences between the quantities disclosed in the two patent applications appear respectively in FIG. 1 thereof, hi-lited copies of which are attached hereto as Exhibit E. Indicative of the differences between the two patent application's disclosed quantities are the facts that:

1. the '282 patent discloses:
  - a. the sender sending three (3) quantities through the insecure channel to the receiver; and
  - b. the receiver sending one (1) quantity through the insecure channel to the sender; while

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

2. the present patent application discloses:
  - a. the sender sending only two (2) quantities through the insecure channel to the receiver; and
  - b. the receiver sending nothing through the insecure channel to the sender.

Consequently, because the '230 patent application discloses quantities different from those disclosed in the present application, the '282 patent does not enable, disclose or suggest the present patent application's claims. For this reason, the '230 patent application provides no basis for rejecting claims 1-29 presently pending in this patent application on the grounds of nonstatutory obviousness-type double patenting over claims 1-41 of the '282 patent.

For the preceding reasons, Applicant respectfully:

1. submits that the claims pending in this patent application traverse rejection on the nonstatutory ground of obviousness-type double patenting over the '282 patent; and
2. requests that the rejection of claims 1-29 based on the nonstatutory ground of obviousness-type double patenting be withdrawn.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

**Claims 1-29 Traverse**  
**Rejection for Obviousness**  
**Based Upon The Crandall Patent**

Based upon the rejection of pending claims 1-29 changing from anticipation under 35 U.S.C. § 102(b) in the January 18, 2005, Office Action to obviousness under 35 U.S.C. § 103(a) in the December 29, 2005 Office Action, and based also upon the comparison of the texts respectively of the January 18, 2005, and December 29, 2005, Office Actions appearing in Exhibit A, Applicant understands that there exists no dispute that the Crandall Patent expressly discloses:

1. the receiver computes using equation (12) and transmits for storage in the public source 813 only a single quantity theirPub<sup>1</sup>;
2. the sender computes using equation (13) and transmits to the receiver, via the public source 813, only a single quantity ourPub<sup>2</sup>; and
3. the "parameters [stored in the public source 813 in addition to theirPub and ourPub] are established for both sender and recipient,"<sup>3</sup> probably by a highly mathematically-skilled, trusted third party.

---

<sup>1</sup> See the Crandall patent at col. 8, lines 8-23.

<sup>2</sup> Ibid.

<sup>3</sup> See the Crandall patent at col. 7, lines 30-31.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

In rejecting pending independent claims 1, 10, 19 and 28 the December 29th Office Action relies upon a conclusory allegation that:

[i]t would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables . . . .

Applicant finds the preceding allegation to be ambiguous because it doesn't specifically identify "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository."

1. Are "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository" quantities in addition to quantities disclosed in the Crandall patent?
2. Are "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository" one or more of the "parameters [stored in the public source 813 in addition to theirPub and ourPub that] are established for both sender and recipient?"

Assuming for sake of argument that "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository" are in

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

addition to quantities disclosed in the Crandall patent, Applicant respectfully submits that to be cryptographically useful such additional, publicly stored quantities require a cryptographic mathematics that differs from the "Elliptic Curve Algebra" disclosed in the Crandall patent. Since the Crandall patent discloses only "Elliptic Curve Algebra" and does not suggest any mathematics in addition to or other than "Elliptic Curve Algebra," the Crandall patent fails to disclose or to suggest the existence of any cryptographically useful additional, publicly storable quantities. Accordingly, under an assumption that "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository" are quantities in addition to quantities disclosed in the Crandall patent, that reference fails to render claims 1-29 obvious under 35 U.S.C. § 103(a).

Alternatively, assuming again for sake of argument that "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository" are one or more of the "parameters [stored in the public source 813 in addition to theirPub and ourPub that] are established for both sender and recipient," there exist at least one technological problem concerning the obviousness of the quantities' storage.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

**How Does "The Receiving Unit" Obtain The Quantities?**

An initial technological problem with the obviousness of the quantities' storage is how would "the receiving unit" obtain the quantities for storage in the publicly accessible repository. There appear to exist only two (2) ways in which "the receiving unit" might obtain the quantities for storage in the publicly accessible repository.

1. "the receiving unit" retrieves the quantities from a place where they have been previously stored.
2. "the receiving unit" receives the quantities directly from whoever generates the quantities.

Either of the two (2) preceding ways in which "the receiving unit" might obtain the quantities for storage in the publicly accessible repository requires that "the receiving unit" either:

1. know in advance the special place where the quantities may be obtained; or
2. know in advance who to contact to receive the quantities.

If "the receiving unit" needs neither of the two (2) types of preceding information, then the quantities must be already available from a publicly accessible repository.

Furthermore, if "the receiving unit" needs to know in advance the special place where the quantities may be obtained, how does "the receiving unit" obtain that information? **If information of**



Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

the special place where the quantities may be obtained is generally, publicly known, then aren't the quantities already effectively available from a publicly accessible repository?

Similarly, if "the receiving unit" needs to know in advance who to contact to receive the quantities, how does "the receiving unit" obtain that information? If information of who "the receiving unit" must to contact to receive the quantities is generally, publicly known, then aren't the quantities already effectively available from a publicly accessible repository?

Thus, the only way in which "the receiving unit" might obtain "the plurality of public quantities" which the December 29th Office Action alleges would be obvious for "the receiving unit" to store in "the publicly accessible repository" that is not from a publicly accessible repository would be if information of who to contact to receive the quantities was secret information known only to "the receiving unit." Under such circumstances, there can exist only one, or a select few, "receiving units" who know who to contact to receive "the plurality of public quantities" which it allegedly would be obvious for "the receiving unit" to store in "the publicly accessible repository." If this were the state of affairs, then no cryptographic communications could occur until the one, or one of the select few, "receiving units" who know who to contact to

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

receive "the plurality of public quantities" acts to make the quantities publicly available.

Clearly, the Crandall patent's disclosure envisions pairs of sending units and receiving units freely communicating cryptographically once both "the receiving unit" and "the sending unit" respectively:

1. compute ourPub and theirPub; and
2. then store ourPub and theirPub into the public source 813.

The Crandall patent's disclosure clearly does not envision no one being able to communicate cryptographically until a particular "receiving unit" having special information acts to make the parameters publicly available. Thus, assuming that "the plurality of public quantities" which the December 29th Office Action alleges would be obvious for "the receiving unit" to store in "the publicly accessible repository" requires action by a "receiving unit" having special information necessarily modifies the Crandall patent to such an extent that it no longer works for its intended purpose, i.e. sending units and receiving units freely communicating cryptographically.

Modifying a reference to such an extent that it no longer works for its intended purpose is an unobvious modification. The reference as so modified can no longer be applied to render a

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

claimed invention obvious. In re Gordon, supra citing Application of Schulpen 390 F.2d 1009, 1013, 157 USPQ 52, 55 (CCPA 1968).

The Manual of Patent Examining Procedure ("MPEP") § 2143.01, Eighth Edition, revised October 2005, at p. 2100-137, in applying the controlling legal authority cited above expressly instructs examiners that claims are not to be rejected for obviousness under 35 U.S.C. § 103(a) relying upon a modification which renders the reference inoperable for the reference's intended purpose. This text in MPEP expressly states as follows.

THE PROPOSED MODIFICATION CANNOT  
RENDER THE PRIOR ART UNSATISFACTORY  
FOR ITS INTENDED PURPOSE

If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984) (Claimed device was a blood filter assembly for use during medical procedures wherein both the inlet and outlet for the blood were located at the bottom end of the filter assembly, and wherein a gas vent was present at the top of the filter assembly. The prior art reference taught a liquid strainer for removing dirt and water from gasoline and other light oils wherein the inlet and outlet were at the top of the device, and wherein a pet-cock (stopcock) was located at the bottom of the device for periodically removing the collected dirt and water. The reference further taught that the separation is assisted by gravity. The Board concluded the claims were prima facie obvious, reasoning that it would have been obvious to turn the reference device upside down. The court reversed, finding that if the prior art device was turned upside down it would be inoperable for its intended purpose because the gasoline to be filtered would be trapped at the top, the water and heavier oils sought to

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

be separated would flow out of the outlet instead of the purified gasoline, and the screen would become clogged.).

Since as explained in greater detail above the modification of the Crandall patent presented in the December 29th Office Action that it would be obvious for "the receiving unit" to store the plurality of public quantities" in "the publicly accessible repository" either:

1. requires using a cryptographic mathematics that differs from the "Elliptic Curve Algebra" disclosed in the Crandall patent; or
2. requires that the quantities be publicly accessible; or
3. renders the Crandall patent inoperable for its intended purpose;

Applicant respectfully:

1. submits that pending claims 1-29 traverse the rejection under 35 U.S.C. § 103(a) for obviousness appearing in the December 29, 2005, Office Action;
2. requests that the rejection be withdrawn; and
3. requests that this patent application pass promptly to issue.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

**Why Pick "The Receiving Unit?"**

Another difficulty with the modification of the Crandall patent presented in the December 29th Office Action that it would be obvious for "the receiving unit" to store the plurality of public quantities" in "the publicly accessible repository" is selecting "the receiving unit" rather than "the sending unit." The rejection of claims 1-29 for obviousness under 35 U.S.C. § 103(a) based upon the Crandall patent fails to explain why it would be obvious "to have the receiving unit transmit the plurality of public quantities . . . ." Why wouldn't it be just as obvious to have "the sending unit," rather than "the receiving unit," transmit the plurality of public quantities . . . .

Applicant suggests that the failure of the obviousness claim rejection based upon the Crandall patent to specifically explain why it would be obvious "to have the receiving unit transmit the plurality of public quantities . . . ," rather than "the sending unit" proves that the Crandall patent lacks any motivation for the modification presented in the Office Action. Although a prior art device "may be capable of being modified to run the way [the inventive] apparatus is claimed, there must be a suggestion or motivation in the reference to do so." In re Mills, supra, In re Naylor, supra, and In re Spormann, supra.

Appl. No. 09/655,229

Response Dated May 1, 2006

Reply to Office Action dated December 29, 2005,

Since there exists no motivation for selecting "the receiving unit" rather than "the sending unit" to store the plurality of public quantities" in "the publicly accessible repository" as alleged in the December 29th Office Action other than the claims now pending in this patent application, Applicant respectfully:

1. submits that pending claims 1-29 traverse the rejection under 35 U.S.C. § 103(a) for obviousness appearing in the December 29, 2005, Office Action;
2. requests that the rejection be withdrawn; and
3. requests that this patent application pass promptly to issue.

### Conclusion

For the reasons set forth above Applicant respectfully submits that claims 1-29 traverse rejection:

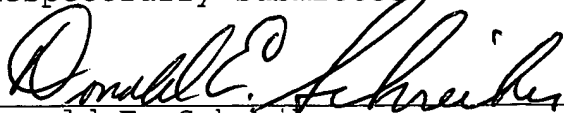
1. for nonstatutory obviousness-type double patenting over claims 1-41 of the '282 patent; and
2. for obviousness under 35 U.S.C. § 103(a) in view of the Crandall patent.

Since claims 1-29 traverse both rejections appearing in the December 29th Office Action, Applicant respectfully requests that:

1. the claim rejections be withdrawn; and
2. this patent application pass promptly to issue.

Appl. No. 09/655,229  
Response Dated May 1, 2006  
Reply to Office Action dated December 29, 2005,

Respectfully submitted

  
Donald E. Schreiber  
Reg. No. 29,435

Dated: 1 May, 2006

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicant

4 5. Claims 1-29 are rejected under 35 U.S.C. ~~102(b)~~ ~~as clearly anticipated by~~ 103(a) as being unpatentable over Crandall U.S. Pat. No. 5805703 (hereinafter Crandall).

6. As per claim 1, Crandall discloses a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted ciphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the ciphertext message M from the communication channel I and by supplying the ciphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom (Crandall: summary: conventional cryptographic communication), a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the ciphertext message M comprising the steps of

~~—— a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities (Crandall: column 20 lines 15-24 and figure 12: store publicly known information);~~

~~b. the sending unit S:~~

~~—— i. retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key);~~



—ii. using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities (Crandall: column 19: lines 42-48: plurality of sender's quantities are ciphertext message and signature); and

—iii. using at least one of the plurality of public quantities, computing the key K (Crandall: column 13 lines 18-30); and

c. the receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S computing the key K (Crandall: figure 12 and column 20 lines 42-52: the using sender's public key to compute deciphering key).

Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

7. As per claim 2, Crandall further discloses the method of claim 1 wherein the receiving unit R, in storing the plurality of public quantities into the publicly accessible repository

(Crandall: column 20 lines 15-24: stores publicly known information):

——~~i.~~ selects at least one receiver's secret quantity (Crandall: column 8 lines 16-20 and figure 3: receiver's public key is produced by using its private key);

——~~ii.~~ selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity (Crandall: column 15 lines 28-33); and

——~~iii.~~ using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (Crandall: column 15 lines 34-38 and column 8 lines 16-20).

8. As per claim 3-5, Crandall further discloses the method of claim 2 wherein the plurality of public quantities/computed public quantities/selected public quantity include a plurality of vectors (Crandall: column 20 lines 15-24: sender's and receiver's public keys and curve parameter..., etc. ; column 8 lines 8-42: how public keys are generated).

9. As per claim 6, Crandall further discloses the method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

——~~i.~~ selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

10. As per claim 7, Crandall further discloses the method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature  $(u,P)$  is sent to the receiver; column 16 - column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

11. As per claim 8, Crandall further discloses the method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

± 12. selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit "R" the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality

of quantities).

13. As per claim 9, Crandall further discloses the method of claim 8 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature  $(u,P)$  is sent to the receiver; column 16 - column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

14. As per claim 10 and 19, Crandall discloses a system adapted for communicating as an encrypted ciphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

——a. a communication channel I adapted for transmitting the ciphertext message M (Crandall: summary: conventional cryptographic communication);

——b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the ciphertext message M from one transceiver to the other transceiver via said communication channel I (Crandall: summary: conventional cryptographic communication); and

——c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the ciphertext message M thereto or receiving the ciphertext message M therefrom (Crandall: summary: conventional cryptographic communication), each cryptographic unit:

——i. when the cryptographic unit is to receive the ciphertext message M:

~~——(1) storing plurality of public quantities in a publicly accessible repository (Crandall: column 20 lines 15-24 and figure 12: store publicly known information);~~

~~(2)~~ receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit (Crandall: column 19: lines 42-48 and figure 12: plurality of sender's quantities are ciphertext message and signature), and using at least one of the plurality of sender's quantities in computing the key K (Crandall: column 13 lines 18-30); and

~~——ii.~~ when the cryptographic unit is to send the ciphertext message M, retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key) and using:

~~——(1)~~ at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit (Crandall: column 19: lines 42-48: plurality of sender's quantities are ciphertext message and signature); and

~~——(2)~~ at least one of the plurality of public quantities in computing the key K (Crandall: column 13 lines 18-30) ; and

~~——iii.~~ including a cryptographic device having:

~~——(1)~~ a key input port for receiving the key K from the cryptographic unit (Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided the key);

—(2) a plaintext port (Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided key along with plaintext):

—(a) for accepting the plaintext message P for encryption into the ciphertext message M that is transmitted from the cryptographic device (Crandall: figure 12 and column 20 lines 25-41: generate ciphertext and send it); and

—(b) for delivering the plaintext message P obtained by decrypting the ciphertext message M received by the cryptographic device (Crandall: column 20 lines 42-52 and figure 12); and

—(3) a ciphertext port that is coupled to one of said transceivers:

—(a) for transmitting the ciphertext message M to such transceiver (Crandall: figure 12: the cryptography device sends the ciphertext), and

—(b) for receiving the ciphertext message M from such transceiver (Crandall: figure 12: the cryptography device receives the ciphertext).

Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the

publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

15. As per claim 11 and 20, Crandall further discloses the system of claims 10 and 19 wherein said cryptographic unit which receives the ciphertext message M in storing the plurality of public quantities into the publicly accessible repository (Crandall: column 20 lines 15-24: stores publicly known information):

——(a) selects at least one receiver's secret quantity (Crandall: column 8 lines 16-20 and figure 3: receiver's public key is produced by using its private key);

——(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity (Crandall: column 15 lines 28-33); and

——(c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (Crandall: column 15 lines 34-38 and column 8 lines 16-20).

16. As per claim 12-14 and 21-23, Crandall further discloses the system of claims 11 and 19 wherein the plurality of public quantities/computed public quantities/selected public quantity include a plurality of vectors (Crandall: column 20 lines 15-24: sender's and receiver's public keys and curve parameter., etc. ; column 8 lines 8-42: how public keys are generated).

17. As per claim 15 and 24, Crandall further discloses the system of claims 11 and 19 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

——i. selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

——ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

18. As per claim 16 and 25, Crandall further discloses the system of claims 15 and 24 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature  $(u, P)$  is sent to the receiver; column 16 - column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

19. As per claim 17 and 26, Crandall further discloses the system of claims 10 and 19 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

——i. selects a sender's secret quantity (Crandall: column 13



lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

20. As per claim 18 and 27, Crandall further discloses the system of claims 17 and 16 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature  $(u,P)$  is sent to the receiver; column 16 - column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

21. As per claim 28, Crandall discloses a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature (Crandall: summary: communication channel; column 19 lines 42-48: send ciphertext and digital signature), and, wherein before transmitting the message M and the digital signature, ~~the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities (Crandall: column 20 lines 15-24: store publicly known information),~~ a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature (Crandall: column 16 lines 63-67: authenticate the digital

signature) comprising the steps performed by the receiving unit R of:

- a. retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 17 lines 1-50);
- b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships (Crandall: column 17 lines 44-50: two different equations); and
- c. comparing pairs, of results obtained by evaluating the expressions of the at least two (2) different verification relationships (Crandall: column 17 lines 49-50: the digital signature is assumed authenticated when Q and R match).

Crandall does not explicitly disclose the transmitting unit 5 transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

22. As per claim 29, Crandall further discloses the method of claim 28 wherein the plurality of public quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the

signature  $(u, P)$  is sent to the receiver; column 16 - column 17:  
two points on the curve; column 8 lines 35-36: form an abelian  
group).



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/655,229	09/05/2000	2131	465	2174	1	29	4

Donald E Schreiber  
Law Office of Donald E Schreiber  
Post Office Box 64150  
Sunnyvale, CA 94088-4150

## FILING RECEIPT



\*OC000000005498019\*

Date Mailed: 10/24/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

## Applicant(s)

Chung Nan Chang, Los Altos, CA ;

## Continuing Data as Claimed by Applicant

## Foreign Applications

If Required, Foreign Filing License Granted 10/23/2000

\*\* SMALL ENTITY \*\*

## Title

Secure cryptographic key exchange and verifiable digital signature

## Preliminary Class

380

Data entry by : RIVERS, ANNETTE

Team : OIPE

Date: 10/24/2000





## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/655,230	09/05/2000	2131	573	2170	1	41	4

Law Office of Donald E Schreiber  
Post Office Box 64150  
Sunnyvale, CA 94088-4150

## FILING RECEIPT



\*OC000000005494645\*

Date Mailed: 10/23/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

## Applicant(s)

Chung Nan Chang, Los Altos, CA ;

## Continuing Data as Claimed by Applicant

## Foreign Applications

If Required, Foreign Filing License Granted 10/21/2000

\*\* SMALL ENTITY \*\*

## Title

Simplified secure, swift cryptographic key exchange

## Preliminary Class :

713

Data entry by : BALL, ROSALIND

Team : OIPE

Date: 10/23/2000



1. In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom, a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:

- a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities;
- b. the sending unit S:
  - i. retrieving the plurality of public quantities from the publicly accessible repository;~~and~~
  - ii. using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities; and
  - iii. using at least one of the plurality of public quantities, computing the key K; and

c. the receiving unit R, using ~~at least some of the plurality of public quantities and~~ at least one of the plurality of sender's quantities received from the sending unit S:

30           ~~i. computing and transmitting to the sending unit S at least one receiver's quantity; and~~

~~ii. computing the key K; and~~

d. ~~the sending unit S, using at least some of the plurality of public quantities and the receiver's quantity received~~  
35       ~~from the receiving unit R, computing the key K.~~

14 10. A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

5 a. a communication channel I adapted for transmitting the cyphertext message M;

b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I; and

10 c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic unit:

15 i. when the cryptographic unit is to receive the cyphertext message M:

(1) storing plurality of public quantities in a publicly accessible repository;

(2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and using at least one of the plurality of sender's quantities ~~and at least some of the plurality of public quantities~~ in computing;

20



- 25                   ~~(a) at least one receiver's quantity which~~  
                      ~~said receiving cryptographic unit~~  
                      ~~transmits via the communication channel I~~  
                      ~~to said sending cryptographic unit; and~~
- ~~(b) the key K; and~~
- 30           ii. when the cryptographic unit is to send the  
              cyphertext message M, retrieving the plurality of  
              public quantities from the publicly accessible  
              repository and using them ~~in computing~~;
- (1) at least some of the plurality of public  
35               quantities in computing the plurality of  
                  sender's quantities which the sending crypto-  
                  graphic unit transmits via the communication  
                  channel I to the receiving cryptographic unit;  
                  and
- 40               (2) ~~after receiving via the communication channel~~  
                  ~~I the receiver's quantity from the receiving~~  
                  ~~cryptographic unit,~~ at least one of the  
                  plurality of public quantities in computing  
                  the key K; and
- 45           iii. including a cryptographic device having:
- (1) a key input port for receiving the key K from  
                      the cryptographic unit;
- (2) a plaintext port:

- 50 (a) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and
- 55 (b) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and
- (3) a cyphertext port that is coupled to one of said transceivers:
- 60 (a) for transmitting the cyphertext message M to such transceiver, and
- (b) for receiving the cyphertext message M from such transceiver.

27 19. A cryptographic unit adapted for inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system including:

- 5 a. a communication channel I adapted for transmitting the cyphertext message M; and
- b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to  
10 the other transceiver via said communication channel I; the cryptographic unit being adapted for coupling to said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, and comprising:
  - a. ports:
    - 15 i. when the cryptographic unit is to receive the cyphertext message M, for:
      - (1) storing plurality of public quantities in a publicly accessible repository;
      - (2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and ~~the receiving cryptographic unit using~~ using at least one  
20 of the plurality of sender's quantities and at least some of the plurality of public  
25 quantities in computing

~~(a) at least one receiver's quantity which  
said receiving cryptographic unit  
transmits via the communication channel I  
to said sending cryptographic unit; and~~

30

~~(b) the key K; and~~

ii. when the cryptographic unit is to send the  
cyphertext message M, for retrieving the plurality  
of public quantities from the publicly accessible  
repository, ~~the sending cryptographic unit using~~  
the retrieved and using:

35

(1) at least some of the plurality of public  
quantities in computing: the plurality of  
sender's quantities which the sending crypto-  
graphic unit transmits via the communication  
channel I to the receiving cryptographic unit;  
and

40

(2) ~~after receiving via the communication channel~~  
~~I the receiver's quantity from the receiving~~  
~~cryptographic unit, at least one of the~~  
plurality of public quantities in computing  
the key K; and

45

b. a cryptographic device having:

i. a key input port for receiving the key K from the  
cryptographic unit;

50

ii. a plaintext port:

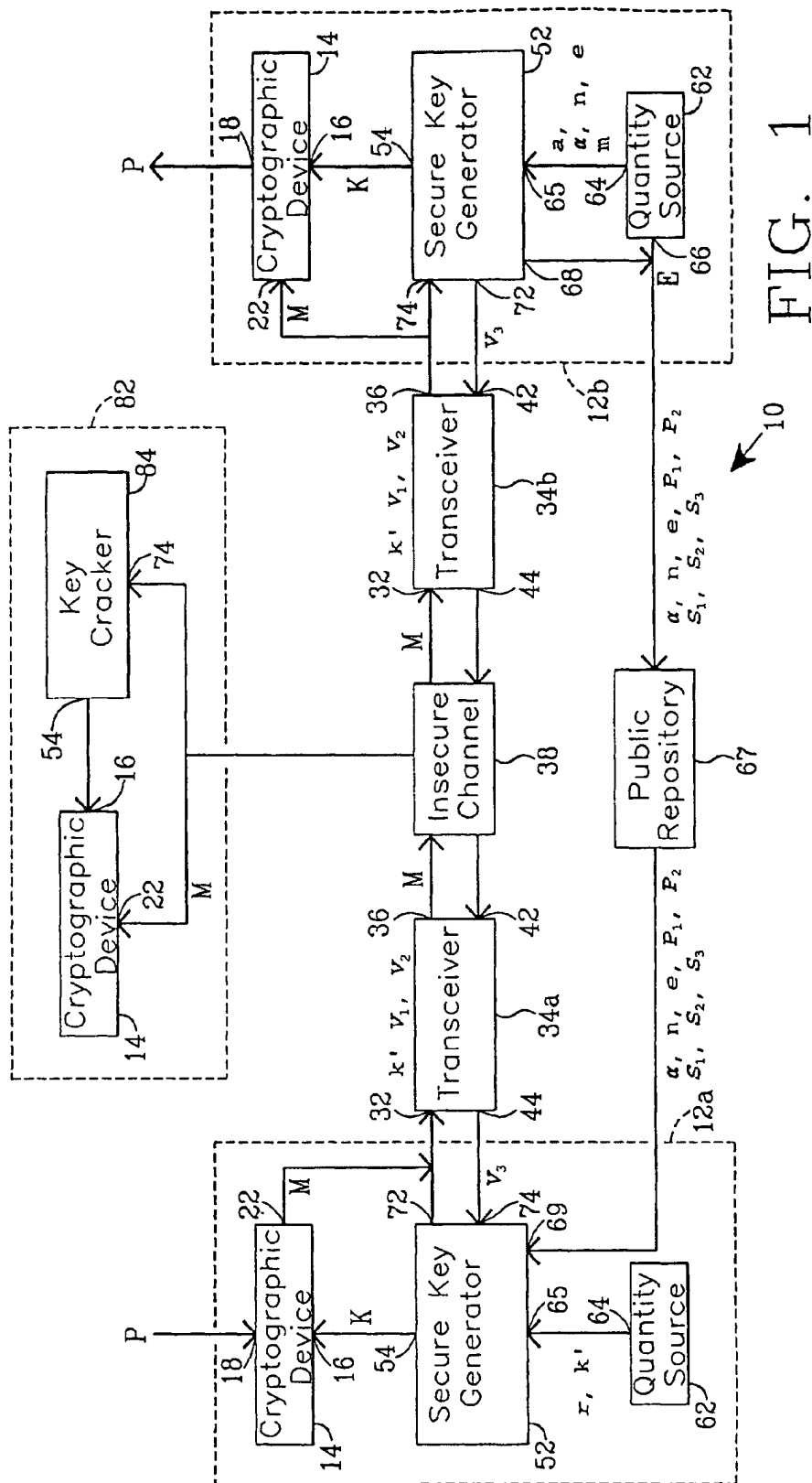
(1) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and

55 (2) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

ii. a cyphertext port that is coupled to one of said transceivers:

60 (1) for transmitting the cyphertext message M to such transceiver, and

(2) for receiving the cyphertext message M from such transceiver.



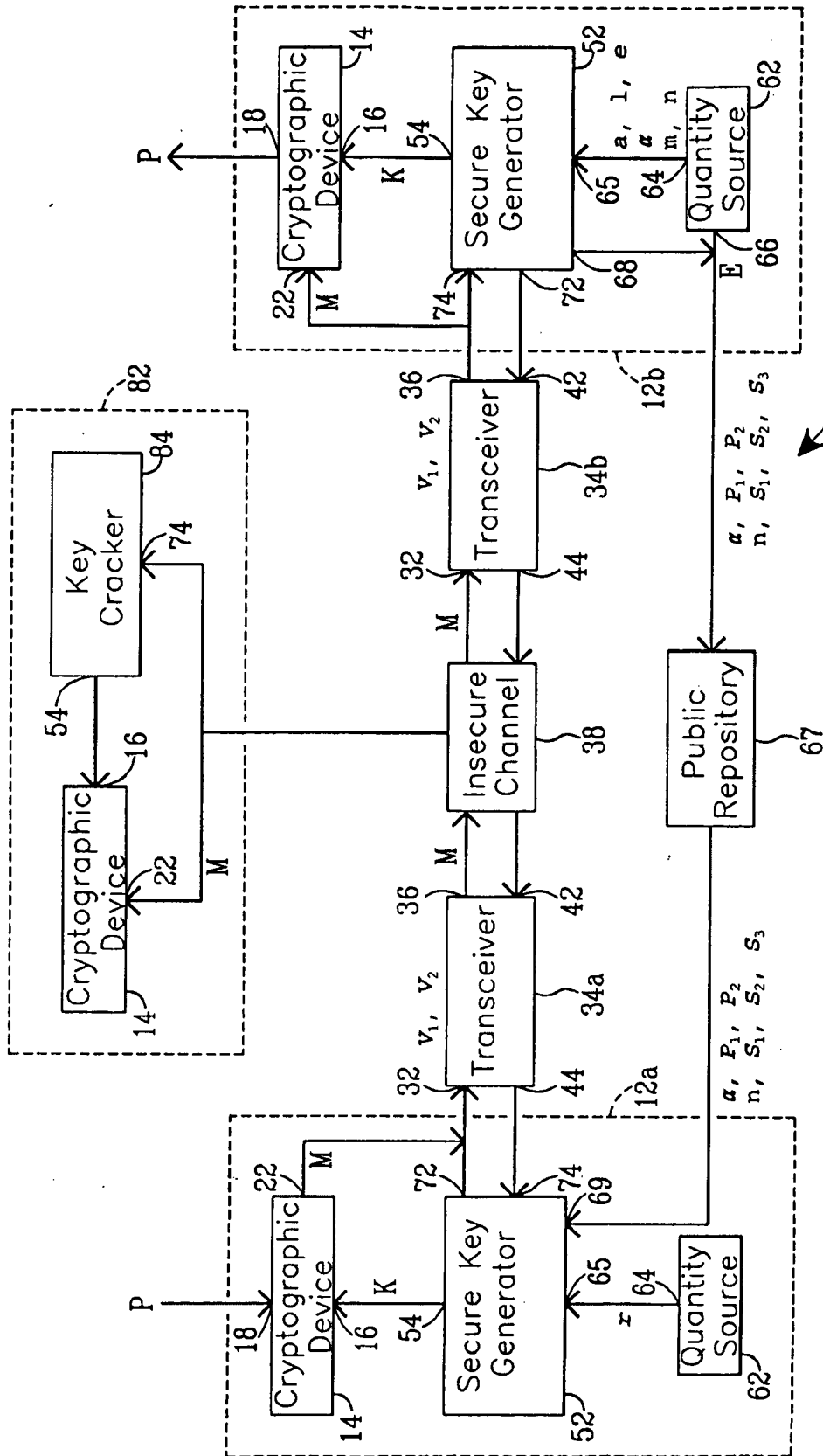


FIG. 1